“phishing”

Tarmo Randel

What it is?

Method of going after information (/money/...)
pretending to be someone else

Why?

- Financial gain
- Preparation for bigger crime
- Breaking trust

Who?

- Whoever has money and/or information
  - Financial institutions (banks, paypal ...)
  - Social networks
  - Popular RPGs (WoW)
  - … ?

Hard to detect and mitigate

- You can get information that you were targeted after the attack
- Information goes “outside” (hotmail e-mail, proxies)
- Lifespan **very** short (2..3 days)
- Timezone difference – take-down: smart crooks prefer timezones +5..8h

Prevention

- They do make mistakes
  - Take control of your referrers
  - Take control of backscatter
  - Monitor logs
- Be prepared:
  - Participate in antiphishing organizations
  - Know, how to report and who to involve

Mitigating

- Find attack vector (search for e-mail, ask communities ...)
- Try to obtain prepared “kit”
  - Usually easy-to-read PHP code, getting worse
  - Look for logfiles, mailto -s
  - / practical exercise /
- Start take-down immediately!
  - Identify and notify ISPs and domain name holders
  - Blacklist 'em all!

Tasks

- Find some antiphishing organizations
- Find some free phishkits (a la just4sec.com, note - some kits are taking advantage of the miscreants ;-))
- Find “kit” in https://sim.cert.ee/phish/ (lowercase, 2 chars, zip archive) /../phish/demo.py